Docket No.: DPO-0007 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of :
:
Myung Dae OH :
:
Serial No.: New U.S. Patent Application :
:
Filed: September 25, 2003 :
:
Customer No.: 34610 :
:
For: METHOD OF CIPHERING DATA AND/OR VOICE CALL TO BE TRANSFERRED IN MOBILE COMMUNICATION SYSTEM AND METHOD OF DEACTIVATING THE CIPHERING

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

U.S. Patent and Trademark Office
2011 South Clark Place
Customer Window
Crystal Plaza Two, Lobby, Room 1B03
Arlington, Virginia 22202

Sir:

At the time the above application was filed, priority was claimed based on the following application:

Korean Patent Application No. 2002-72008 filed November 19, 2002

A copy of each priority application listed above is enclosed.

Respectfully submitted,
FLESHNER & KIM, LLP

Daniel Y.J. Kim
Registration No. 36,186
Samuel W. Ntiros
Registration No. 39,318

P.O. Box 221200
Chantilly, Virginia 20153-1200
703 502-9440 DYK/SWN:jab
Date: September 25, 2003

Please direct all correspondence to Customer Number 34610

대 한 민 국 특 허 청

KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0072008
Application Number

출 원 년 월 일 : 2002년 11월 19일
Date of Application NOV 19, 2002

출 원 인 : 엘지전자 주식회사
Applicant(s) LG Electronics Inc.

2003 년 03 월 21 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2002.11.19
【국제특허분류】	H04B 1/00
【발명의 명칭】	ＧＳＭ이동통신 시스템의 전송 데이타 암호화 및 암호화 해제 방법
【발명의 영문명칭】	Method for activate ciphering the transfor data of mobile system for GSM and deactivate cipering the same
【출원인】	
【명칭】	엘지전자 주식회사
【출원인코드】	1-2002-012840-3
【대리인】	
【성명】	양순석
【대리인코드】	9-1998-000348-9
【포괄위임등록번호】	2002-027111-1
【발명자】	
【성명의 국문표기】	오명대
【성명의 영문표기】	OH,MYUNG DAE
【주민등록번호】	741231-1781710
【우편번호】	157-016
【주소】	서울특별시 강서구 화곡6동 한양아파트 B동 202호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 양순석 (인)
【수수료】	
【기본출원료】	20 면 29,000 .원
【가산출원료】	15 면 15,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	18 항 685,000 원
【합계】	729,000 원

1020020072008

출력 일자: 2003/3/27

【첨부서류】

1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 GSM 이동통신 시스템에서 단말기와 네트워크간의 전송되는 데이타 및 음성 콜을 암호화 및 암호화 해제 하고자 할때 이를 GSM 이동통신 단말기에서 직접 하기위한 방법에 관한 것이다.

이를 위하여 본 발명은 단말기와 네트워크간에 테이타 전송중 암호화가 필요하면 사용자 단말기는 네트워크에 전송되는 메시지의 암호화를 요청하는 전송중 암호와 메시지 요청단계와, 상기 네트워크는 단말기로 부터 온 전송중 암호화 메시지 요청을 받아 이를 승인하는 메시지를 상기 단말기로 전송해주는 암호화 요청 메시지 승인단계와, 상기 단말기는 네트워크로 부터 온 암호화 요청 메시지 승인에 따라 이에 응답하는 메시지를 네트워크로 전송해주는 암호화 승인 메시지 응답단계와, 상기 네트워크는 단말기로 부터 온 암호화 승인 응답 메시지에 따라 데이타 전송중 암호화가 완료 되었다는 메시지를 단말기로 보내주는 전송중 암호화 메시지 완료단계를 포함하여 이루어지고, 단말기와 네트워크간에 테이타 전송중 암호화가 필요없으면 사용자 단말기는 네트워크에 전송되는 메시지의 암호화 해제를 요청하는 전송중 암호와 해제 메시지 요청단계와, 상기 네트워크는 단말기로 부터 온 암호화 해제 요청 메시지를 받아 이를 처리하여 승인하는 전송중 암호화 중단 완료 메시지를 상기 단말기로 전송해주는 암호화 중단완료 메시지 승인단계를 포함하여 이루어진 것으로 사용자는 아무때나 데이타 전송을 원하는 시점부터 데이타를 암호화 하거나 암호화를 해제하거나 함으로써 전송되는 데이타의 신뢰성을 그만큼 높여주는 효과를 제공해준다.

【대표도】

도 8a

【색인어】

GSM 단말기, 암호화

【명세서】

【발명의 명칭】

G S M 이동통신 시스템의 전송 데이타 암호화 및 암호화 해제 방법{Method for activate ciphering the transfor data of mobile system for GSM and deactivate ciperin the same}

【도면의 간단한 설명】

도 1 은 GSM 이동통신 단말기의 전송 데이타 암호화 과정을 도시한 통상의 개략적인 시스템 구성도.

도 2 는 종래의 GSM 이동통신 단말기와 네트워크 사이에서 암호화 과정 중에 이루어 지는 메시지 흐름도.

도 3 은 종래의 GSM 이동통신 단말기가 음성 콜을 하기 위해 수행하는 절차에 대해서 나타낸 메시지 흐름도.

도 4 는 종래의 GSM 이동통신 시스템에서 암호화 과정을 나타내는 플로우 차트.

도 5 는 본 발명의 GSM 이동통신 시스템에서 암호화 과정을 나타내는 시스템 동작 흐름도.

도 6 은 본 발명의 GSM 이동통신 시스템에서 특정 키 값에 따라 암호화 과정을 나타내는 시스템 동작 흐름도.

도 7 은 본 발명의 GSM 이동통신 시스템에서 암호화 해제과정을 나타내는 동작 흐름도.

도 8 은 본 발명의 GSM 이동통신 시스템에서 암호화 과정을 나타내는 플로우 차트.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<9> 본 발명은 이동통신 시스템에서 데이타 전송시 이를 암호화 및 암호화를 해제하는 방법에 관한 것으로, 특히 GSM 이동통신 시스템에서 단말기와 네트워크간의 전송되는 데이타 및 음성 콜을 암호화 및 암호화 해제 하고자 할때 이를 GSM 이동통신 단말기에서 직접 하기위한 GSM 이동통신 시스템의 전송 데이타 암호화 및 암호화 해제 방법에 관한 것이다.

<10> 현재 유럽에서 2세대 이동통신 시스템으로 상용 서비스중인 GSM(Global Systems for Mobile communication)과 2.5세대 이동통신 시스템으로 상용 서비스중인 GPRS(General Packet Radio Service)의 경우 사용자 인증 및 암호화 절차를 사용하고 있다.

<11> 상기 사용자 인증 및 암호화 절차는 이동통신 단말기의 전원이 온 될때마다 단말기는 무조건 네트워크에 단말기를 이제부터 사용하겠다는 사용자의 의사표현인 등록절차를 필히 받아야만 한다.

<12> 상기 등록절차에는 부가(Attach) 등록절차와 위치 지역 업데이트(Location Area Update) 등록절차 및 경로 지역 업데이트(Routing Area Update) 등록절차 등이 있다.

<13> 상기한 등록절차들을 거치면서 그 과정중에 네트워크에서 필료시 사용자 인증 및 암호화 과정을 거치고 있다.

<14> 상기와 같이 사용자 인증 및 암호화 과정을 네트워크에서 실행함으로써 단말기 (MS:Mobile Station)는 네트워크에 등록을 요청하게 되면 네트워크에서는 해당 단말기가

인증된 단말기 인지를 확인하는 인증절차(Authentication)와, 단말기와 네트워크간 전송되는 데이타를 암호화 할 지를 결정하는 암호화 절차(Ciphering)를 거치게 된다.

<15> 상기와 같은 인증절차 및 암호화 절차는 전송되는 무선 음성이나 무선 데이타를 타인에 의해 도청 및 악용되는 사례를 방지하기 위한 절차라고 할 수 있다.

<16> 만약 단말기와 네트워크간에 서로 암호화 절차를 통해 암호화가 결정되게 되면 서로간에 전송되는 데이타는 서로의 약속에 의해 암호화 되어진 상태로 전송이 이루어지게 된다.

<17> 이러한 암호화를 할것인지 하지 않을 것인지는 두 가지 방법에 의해 결정이 된다.

<18> 첫째는, 단말기의 전원이 켜지고 난 후 네트워크에 등록하는 과정 중에 일어나는 것이다.

<19> 두 번째는, 단말기가 특정 서비스를 하기를 원하는 시점에 이루어 지는 것이다.

<20> 상기 특정 서비스라고 하면 음성 통화를 위한 음성 콜(Voice call)과, 단문전송을 위한 SMS(Short message service), 부가 서비스를 위한 SS(Supplementary Service), GPRS 패킷 전송을 위한 PDP 컨택스트 액티베이션(Packet Data Protocol Context Activation) 등이 이에 속하게 된다.

<21> 상기의 경우 단말기와 네트워크간에 데이타 전송 과정이 약속이 되어있지 않은 경우, 즉 네트워크 등록시 암호화와 관련한 절차가 이루어 지지 않아서 데이타를 암호화 하지 않고 전송되는 경우라 할지라도 서비스가 이루어지는 시점에서 네트워크에 의하여 암호화와 관련된 절차가 이루어질 수 있다.

<22> 이렇게 되면 단말기와 네트워크는 이 시점부터 전송되는 데이타를 암호화 한 후 전송하게 된다.

<23> 상기와 같은 GSM 이동통신 단말기의 전송 데이타 암호화 기술에 있어서, 통상의 개략적인 시스템 구성은 도 1 에 나타낸 바와 같다.

<24> 상기 도 1 에서 사용자가 통상적으로 사용하는 이동통신 단말기(10)가 구비되고, 단말기(10)와 음성 및 데이타를 주고받는 다수개의 기지국(11)이 있으며, 다수개의 기지국(11)들을 총괄 제어해주는 기지국 제어장치(12)가 있고, 기지국 제어장치(12)와 연결된 교환장치(13)로 이루어져 있다.

<25> 상기 교환장치(13)는 기존의 2세대 서비스인 GSM의 경우에는 MSC(Mobile Switching Center)로 표현할 수 있으며, 2.5세대 서비스인 GPRS이 경우에는 SGSN(Serving GPRS Support Node)으로 표현할 수 있다.

<26> 도 2 는 종래의 GSM 이동통신 단말기와 네트워크 사이에서 암호화 과정 중에 이루어 지는 메시지 흐름도이다.

<27> 유럽에서 상용화 서비스 중인 GSM과 GPRS의 경우 이동통신 단말기의 전원이 온(ON)되면 단말기(10)는 네트워크(20)에게 등록을 요청하게 된다.

<28> 이때 이동통신 단말기(10)는 등록 요청 메시지(Attach Request)(201)를 무선을 통해 기지국(11)으로 전송하게 되고, 기지국(11)은 상기 등록 요청 메시지(201)를 기지국 제어장치(12)를 통해 교환장치(13)로 전송하게 된다.

<29> 상기 네트워크(20)는 단말기(10)로 부터 등록 요청 메시지(201)를 받아서 암호화를 사용할지 여부를 결정하게 되고, 암호화를 사용한다고 결정한 경우 암호화 승인 요청 메시지(Authentication and Ciphering Request)(202)를 단말기(10)로 전송하게 된다.

<30> 상기 단말기(10)는 네트워크(20)로 부터 받은 상기 암호화 승인 요청 메시지(202)에 대응하여 적절한 암호화 승인 응답 메시지(Authentication and Ciphering Response)(203)를 네트워크(20)에 전송 한다.

<31> 상기 네트워크(20)는 단말기(10)로 부터 상기 암호화 승인 응답 메시지(203)을 받은 후 등록절차를 완료하였다는 등록완료 메시지(Attach Accept)(204)를 상기 단말기(10)에게 보내주게 됨으로써 단말기(10)와 네트워크(20)간의 암호화를 위한 과정은 완료가 된다.

<32> 반면에 상기 네트워크(20)에서 암호화를 하지 않기로 결정하게 되면 네트워크(20)는 암호화 메시지를 상기 단말기(10)에게 보내지 않게 되고 또한 단말기(10)와 네트워크(20)간에 데이타는 암호화 되지 않은 상태로 전송이 이루어지게 된다.

<33> 상기와 같은 단말기(10)와 네트워크(20)간에 데이타의 암호화 과정은 초기 등록 절차에서 진행되지 않았더라도 서비스를 사용하는 시점에 네트워크(20)에 의하여 상기 암호화 과정이 수행될 수 있다.

<34> 도 3 은 단말기가 음성 콜(Voice call)을 하기 위해 수행하는 절차에 대해서 나타낸 것이다.

<35> 상기 단말기(10)가 음성 콜을 하기 위해 네트워크(20)에 CM 서비스 요청 메시지(CM Service Request)(301)를 전송 하게 되면 네트워크(20)는 상기 CM 서비스 요청 메시지(301) 중에 암호화를 진행할지 여부를 결정하게 되고 암호화를 진행하고자 한다면 암호화 승인 요청 메시지(Authentication and Ciphering Request)(302)를 단말기(10)로 전송하게 된다.

<36> 여기에서 상기 CM은 Connection Management의 약어이다.

<37> 상기 단말기(10)는 네트워크(20)로 부터 받은 상기 암호화 승인 요청 메시지(302)에 적절한 암호화 승인 응답 메시지(Authentication and Ciphering Response)(303)를 네트워크(20)에 전송 함으로써 단말기(10)와 네트워크(20)간의 암호화를 위한 과정은 완료가 된다.

<38> 상기 네트워크(20)는 단말기(10)로 부터 상기 암호화 승인 응답 메시지(303)를 전송 받은 후 등록절차를 완료하였다는 CM 서비스 등록완료 메시지(CM Service Accept)(304)를 상기 단말기(10)에게 보내주게 된다.

<39> 상기한 종래의 과정을 도 4 를 참조하여 성명하면 다음과 같다.

<40> GSM 방식의 이동통신 단말기에 전원이 켜지고 대기상태(401)에서 단말기는 데이타와 관련된 네트워크에 등록 요청 메시지나 또는 음성 콜과 관련된 CM 서비스요청 메시지를 전송하면 상기 네트워크는 이 메시지를 수신(402)한 다음 암호화를 진행할 것인지 판단(403)한다.

<41> 상기 암호화 진행여부 판단(403) 결과 암호화를 진행하지 않기로 하였으면 암호화를 하지 않겠다는 등록/CM 서비스 완료 메시지를 단말기로 전송(404)하고, 암호화를 진행하지 않는 절차를 완료(405)한다.

<42> 그러면 상기 절차 후 전송되는 모든 데이타는 암호화 되지않은 상태로 전송된다.

<43> 상기 암호화 진행여부 판단(403) 결과 암호화를 진행하기로 하였으면 RAND(RANDom number) 값을 생성하여 SRES(Signed RESponse) 값을 계산/저장(406) 한 다음 암호화 승인 요청 메시지를 단말기로 전송(407)한다.

<44> 상기 단말기는 네트워크로 부터 상기 암호화 승인 요청 메시지를 수신한 다음 암호화 승인 응답 메시지를 네트워크로 전송하면, 상기 네트워크는 단말기로 부터 상기 암호화 승인 응답 메시지를 수신(408)한다.

<45> 상기 네트워크는 단말기로 부터 상기 암호화 승인 응답 메시지를 받아서 네트워크에 저장된 SRES 값과 상기 단말기로 부터 전송된 SRES 값을 비교한 후 서로 두 값이 동일한지 판단(409)한다.

<46> 상기 판단(409) 결과 두 값이 서로 동일하지 않으면 등록/CM 서비스를 더이상 사용할 수 없다는 등록/CM 서비스 불가 메시지를 단말기로 전송(410)한 후 절차를 완료(411)한다.

<47> 상기 절차 완료(411) 후에는 각종 전송 데이타에 암호화 서비스가 불가능하다.

<48> 상기 판단(409) 결과 두 값이 서로 동일하면 등록/CM 서비스를 얼마든지 사용할 수 있다는 등록/CM 서비스 가능 메시지를 단말기로 전송(412)한 후 절차를 완료(413)한다.

<49> 상기 절차 완료(413) 후에는 각종 전송되는 데이타는 암호화되어 서비스가 가능하다.

<50> 이상과 같이 동작하여 음성 콜 과정에서 암호화를 위한 동작이 모두 완료된다.

<51> 상기와 같은 종래의 기술은 암호화 절차를 결정함에 있어서 일방적으로 네트워크에 의해서만 오로지 결정이 이루어진다.

<52> 따라서 초기에 암호화 절차가 이루어지지 않거나 특정 데이타가 아니면 보통의 데이타 전송중 사용자가 중요한 데이타가 있어서 이를 암호화 한 후 전송하기를 원하더라도 암호화를 전혀 진행할 방법이 없게되는 문제점이 있다.

<53> 이 때문에 사용자의 중요한 데이타가 외부에 도청 및 악용될 소지가 발생하게 된다.

<54> 상기 데이타 뿐만 아니라 음성의 경우에도 암호화 되지않고 전송하게 됨으로써 사용자의 중요한 정보들이 모두 타인에게 누출될 수 있는 심각한 문제점이 있다.

【발명이 이루고자 하는 기술적 과제】

<55> 따라서, 본 발명은 상기한 종래의 문제점을 해결하기 위하여 제안한 것으로, GSM 이동통신 시스템에서 단말기와 네트워크간의 전송되는 데이타 및 음성 콜에 암호화를 하거나 암호화를 해제할때 이를 이동통신 사용자 단말기에서 직접 하기위한 GSM 이동통신 시스템의 전송 데이타 암호화 및 암호화 해제 방법을 제공함에 그 목적이 있다.

<56> 상기한 목적을 달성하기 위하여 본 발명은 GSM 이동통신 시스템에서 단말기와 네트워크간의 전송되는 데이타 및 음성 콜에 암호화를 할때 이를 이동통신 단말기에서 직접 암호화를 하되 초기 네트워크 등록이나 혹은 서비스 시작 부분에 단말기와 네트워크간 암호화를 위한 과정이 이루어지지 않을 수 있다.

<57> 이런 경우 단말기를 사용하는 사용자가 만약 자신의 음성이나 혹은 데이타의 중요성에 따라 특정 시점부터 암호화 하기를 원하는 경우 네트워크로 소정의 암호화 절차를 진행하자고 요청을 하게된다.

<58> 상기 네트워크는 단말기 측으로 부터 온 특정시점 암호화 요청에 따라 2가지 방법에 따라 소정의 암호화를 위한 과정을 수행하게 된다.

<59> 첫째는, 단말기가 암호화 과정을 진행하자고 요청할때 통상의 방법으로 네트워크에 의하여 암호화를 위한 과정을 수행하게 된다.

<60> 둘째는, 단말기가 암호화를 요청 하면서 특정 값을 포함해서 보내게되면 그 특정 값을 바탕으로 암호화 과정에 필요한 키 값을 계산한 후 암호화 과정이 완료되었다고 통보를 하게 되고 이때부터 단말기와 네트워크는 암호화를 시작하게 된다.

<61> 또한 사용자가 중요 데이타를 전송 완료하고 더이상 암호화를 원하지 않을 경우 암호화를 중단하자는 메시지를 네트워크로 보낸다.

<62> 그러면 상기 네트워크에서는 그에 따른 응답을 단말기로 보냄으로써 단말기와 네트워크간 암호화 과정은 더이상 이루어지지 않는다.

<63> 본 발명에서 GSM방식의 단말기와 네트워크간에 전송되는 테이타를 암호화 시키는 방법에 있어서,

<64> 상기 단말기와 네트워크간에 테이타 전송중 암호화가 필요하면 사용자 단말기는 네트워크에 전송되는 메시지의 암호화를 요청하는 전송중 암호와 메시지 요청단계와,

<65> 상기 네트워크는 단말기로 부터 온 전송중 암호화 메시지 요청을 받아 이를 승인하는 메시지를 상기 단말기로 전송해주는 암호화 요청 메시지 승인단계와,

<66> 상기 단말기는 네트워크로 부터 온 암호화 요청 메시지 승인에 따라 이에 응답하는 메시지를 네트워크로 전송해주는 암호화 승인 메시지 응답단계와,

<67> 상기 네트워크는 단말기로 부터 온 암호화 승인 응답 메시지에 따라 데이타 전송중 암호화가 완료 되었다는 메시지를 단말기로 보내주는 전송중 암호화 메시지 완료단계를 포함하여 이루어진다.

<68> 상기 사용자 단말기가 네트워크에 요청한 전송되는 메시지의 암호화 요청 메시지 속에는 RAND 값에 의한 키(Kc)값이 생성되어 포함되어 있으며,

<69> 상기 사용자 단말기가 네트워크에 요청한 데이타 전송중 암호와 메시지 요청 시점은 불특정 시점에 하도록 하되 단말기와 네트워크간에 데이타가 전송되는 중간에 요청할 수 있도록 하고,

<70> 상기 사용자 단말기가 네트워크에 요청한 데이타 전송중 암호와 메시지 요청은 단말기와 네트워크간에 전송되는 데이타가 없을 경우에도 이루어 지도록한다.

<71> 상기 단말기가 암호화를 요청 하면서 특정 값을 포함해서 보내고,

<72> 상기 특정 값을 바탕으로 암호화 과정에 필요한 키 값을 계산한 후 암호화 과정이 완료되었다고 통보를 하며,

<73> 상기 통보 후 단말기와 네트워크는 암호화를 시작하게 된다.

<74> 또한, 본 발명은 단말기가 대기상태 또는 전송상태에서 단말기가 네트워크에 지금부터 전송되는 모든 데이타에 암호화를 시작하자고 요청하는 전송중 암호화 요청 메시지 전송단계와,

<75> 상기 네트워크는 상기 전송중 암호화 요청 메시지를 받아 이 메시지속에 RAND 값이 포함되었으면 상기 RAND 값을 이용하여 암호화에 필요한 키(Kc)값을 계산한 다음 전송데이타의 암호화를 완료하는 키값 산출단계와,

<76> 상기 네트워크는 상기 전송중 암호화 요청 메시지를 받아 이 메시지속에 RAND 값이 포함되어있지 않으면 암호화 진행 여부에 따라 RAND 값을 생성하고 SRES 값을 계산/저장한 다음 암호화가 이루어 졌다는 메시지를 단말기로 전송하는 암호화 승인 메시지 전송단계와,

<77> 상기 네트워크는 단말기로 부터 암호화 승인 응답 메시지를 받아 네트워크에 저장된 SRES 값과 단말기에서 전송되어온 SRES 값을 비교하여 동일여부에 따라 전송되는 데이타에 암호화여부를 결정하는 전송데이타 암호화 결정단계를 포함하여 이루어진다.

<78> 상기 단말기의 전송중 암호화 요청 메시지를 네트워크로 전송시 단말기는 이미 RAND 값을 기준으로 하여 암호화를 하기위한 키(KC) 값을 생성 완료하고 암호화 준비를 마치도록 하고,

<79> 상기 네트워크가 단말기로 전송하는 암호화 승인 메시지 속에는 RAND 값이 포함되도록 하며,

<80> 상기 네트워크가 단말기로 부터 수신하는 암호화 승인 응답 메시지 속에는 단말기에서 계산한 SRES 값이 포함된다.

<81> 여기에서, 상기 네트워크는 수신된 전송중 암호화 요청 메시지속에 RAND 값이 포함되어 있지 않고,

<82> 암호화도 진행하지 않기로 하였으면 전송되는 데이타는 암호화가되지 않는다는 메시지를 단말기로 전송하는 암호화 불가 메시지 전송단계를 더 포함하여 이루어진다.

<83> GSM방식의 단말기와 네트워크간에 전송되는 데이타를 암호화 해제 시키는 방법에 있어서,

<84> 상기 단말기와 네트워크간에 데이타 전송중 암호화가 필요없으면 사용자 단말기는 네트워크에 전송되는 메시지의 암호화 해제를 요청하는 전송중 암호와 해제 메시지 요청단계와,

<85> 상기 네트워크는 단말기로 부터 온 암호화 해제 메시지 요청을 받아 이를 처리하여 승인하는 전송중 암호화 중단 완료 메시지를 상기 단말기로 전송해주는 암호화 중단완료 메시지 승인단계를 포함하여 이루어진다.

<86> 상기 사용자 단말기가 네트워크에 요청한 데이타 전송중 암호와 해제 메시지 요청 시점은 불특정 시점으로 하되 단말기와 네트워크간에 데이타가 전송되는 중간에 요청할 수 있도록 하고,

<87> 상기 사용자 단말기가 네트워크에 요청한 데이타 전송중 암호와 해제 메시지 요청은 단말기와 네트워크간에 전송되는 데이타가 없을 경우에도 이루어 지도록 한다

【발명의 구성 및 작용】

<88> 이하 첨부된 도면을 참조하여 본 발명의 실시예를 상세히 설명하면 단음과 같다.

<89> 도 5 는 본 발명의 일 실시예를 나타내는 GSM 이동통신 시스템에서 암호화 과정을 나타내는 동작 흐름도이다.

<90> 이하 본 발명에서 설명되는 실시예는 단말기와 네트워크간 주고 받는 사용자 데이타를 기준으로 설명 하지만 이 외에도 사용자가 전송하는 사용자 음성 콜 메시지도 모두 상기 사용자 데이타속에 포함하는 개념이다.

<91> 상기 사용자 음성 콜 메시지의 전송중 암호화 및 암호화 해제 방법과, 상기 사용자 테이타의 전송중 암호화 및 암호화 해제 방법이 동일 함으로 그중 사용자 데이타를 기준으로 설명한다.

<92> 상기 도 5 에서 사용자가 단말기(10)의 전원을 온 시키면 단말기(10)는 네트워크(20)에게 등록을 요청하게 된다.

<93> 상기 이동통신 단말기(10)는 등록 요청 메시지(Attach Request)(501)를 무선을 통해 네트워크(20) 기지국(11)으로 전송하게 되고, 기지국(11)은 상기 등록 요청 메시지(501)를 기지국 제어장치(12)를 통해 교환장치(13)로 전송하게 된다.

<94> 상기 네트워크(20)는 단말기(10)로 부터 등록 요청 메시지(501)를 받아서 암호화를 사용할지 여부를 결정하게 되고, 암호화를 사용한다고 결정한 경우 암호화 승인 요청 메시지(Authentication and Ciphering Request)(502)를 단말기(10)로 전송하게 된다.

<95> 상기 단말기(10)는 네트워크(20)로 부터 받은 상기 암호화 승인 요청 메시지(502)에 적절한 암호화 승인 응답 메시지(Authentication and Ciphering Response)(503)를 네트워크(20)로 전송한다.

<96> 상기 네트워크(20)는 단말기(10)로 부터 상기 암호화 승인 응답 메시지(503)를 전송 받은 후 등록절차를 완료 하였다는 등록완료 메시지(Attach Accept)(504)를 상기 단말기(10)에게 보내주게 됨으로써 단말기(10)와 네트워크(20)간의 암호화를 위한 초기 과정은 완료가 된다.

<97> 이때, 만약에 상기 네트워크(20)에서 암호화를 하지 않기로 결정하게 되면 네트워크(20)는 암호화 메시지를 상기 단말기(10)에게 보내지 않게 되고 또한 단말기(10)와 네트워크(20)간에 데이타는 암호화 되지 않은 상태로 보통의 전송(505)이 이루어지게 된다.

<98> 상기와 같은 단말기(10)와 네트워크(20)간에 데이타는 암호화 과정이 초기 등록 절차에서 진행되지 않고 데이타를 전송하는 과정(505)에 사용자가 단말기(10)를 통하여 데이타 전송중 전송되는 데이타에 암호화를 할 필료가 있을 경우 사용자 단말기(10)는 데이타

전송중 암호화를 요청하는 메시지(Activate Ciphering Request)(506)를 네트워크(20)로 전송하게 된다.

<99> 이때 상기 데이타 전송중 암호화를 요청하는 메시지(506) 속에는 특정값(RAND : RANDom number)을 포함하지 않고 네트워크(20)로 전송하게 된다.

<100> 상기 네트워크(20)는 단말기(10)로 부터 상기 데이타 전송중 암호화 요청 메시지(506)를 받아서 암호화를 위한 과정을 수행하게 된다.

<101> 상기 네트워크(20)에서 암호화 과정을 마치게되면 네트워크(20)는 단말기(10)에게 암호화에 필요한 암호화 승인 요청 메시지(Authentication and Ciphering Request)(507)를 전송하게 된다.

<102> 상기 단말기(10)는 네트워크(20)로 부터 받은 상기 암호화 승인 요청 메시지(507)에 대한 응답으로 암호화 승인 응답 메시지(Authentication and Ciphering Response)(508)를 네트워크(20)로 보내주게 된다.

<103> 상기 단말기(10)가 네트워크(20)로 암호화 승인 응답 메시지(508)를 보내주면 상기 네트워크(20)는 데이타 전송중 암호화 과정이 모두 완료 되었다는 데이타 전송중 암호화 완료메시지(509)를 단말기(10)로 전송해 줌으로써 암호화 과정에 필요한 모든 절차가 완료되게 된다.

<104> 상기와 같이 데이타 전송중 암호화 과정에 필요한 모든 절차가 완료된 이후로는 전송되는 모든 데이타는 암호화가 되어 전송이 된다.

<105> 도 6 은 상기 단말기(10)로 부터 네트워크(20)로 데이타 전송중 암호화를 요청하는 메시지(601) 속에 특정값(RAND : RANDom number)을 포함하고 네트워크(20)로 전송하게 된다.

<106> 그러면 상기 네트워크(2)는 단말기(10)가 보내온 상기 RAND 특정값을 바탕으로 하여 암호화 과정에 필요한 키(Key) 값을 생성한 다음, 상기 단말기(10)에게 암호화 과정이 완료 되었다는 데이타 전송중 암호화 완료 메시지(602)를 보내주게 된다.

<107> 상기 데이타 전송중 암호화 완료 메시지(602) 전송 이후로는 단말기(10)와 네트워크(20)간 전송되는 모든 데이타는 암호화가 되어 전송이 되게 된다.

<108> 여기에서 상기 단말기(10)가 데이타 전송중 암호화를 요청하는 메시지를 보내는 시점은 다양하게 변할 수 있으며, 단말기(10)와 네트워크(20)간의 데이타가 전송되는 중간에 암호화를 요청하여 이루어질 수도 있고, 단말기(10)와 네트워크(20)간의 전송되는 데이타가 없을 경우에도 암호화를 요청하여 이루어질 수도 있다.

<109> 또한, 단말기(10)와 네트워크(20)간에 암호화가 이루어져서 암호화가 된 데이타가 전송되고 있는 중이라도 단말기 사용자가 더이상 암호화 전송을 원하지 않을 경우 도 7 에 나타낸 바와 같이 단말기 사용자는 단말기(10)를 통해 암호화를 중단 하자는 데이타 전송중 암호화 해제 요청 메시지(Deactivate Ciphering Request)(701)를 네트워크(20)로 전송한다.

<110> 상기 단말기가 네트워크로 전송하는 암호화 해제 메시지는 단말기에 의해서 전송되는 데이타속에 이미 암호화가 해제된 데이타가 포함되어 전송되고 있음을 의미한다.

<111> 상기 네크워크(20)는 단말기(10)로 부터 상기 데이타 전송중 암호화 해제 요청 메시지(701)를 받고난 후 상기 데이타 전송중 암호화 해제 요청 메시지(701)에 상응하는 데이타 전송중 암호화 해제 완료 메시지(Deactivate Ciphering Complete)(702)를 단말기(10)에게 전송 함으로써 지금까지 이루어진 암호화 과정을 모두 해제하게 된다.

<112> 도 8 의 (A)도와 (B)도는 본 발명의 GSM 이동통신 시스템에서 암호화 과정을 나타내는 플로우 차트이다.

<113> GSM 방식의 이동통신 단말기가 대기상태나 또는 데이타 전송상태(801)에서 단말기는 데이타 전송중 암호화 요청 메시지를 네트워크로 전송해주면, 상기 네트워크는 단말기로 부터 상기 데이타 전송중 암호화 요청 메시지를 수신(802)한 다음 수신된 메시지에 RAND 값이 포함 되어있는지 판단(803)한다.

<114> 본 발명에서 상기 단말기가 데이타 전송중 암호화 요청 메시지를 네트워크로 전송해주었다는 의미는 본 발명의 단말기가 이미 RAND 값을 기준으로 하여 암호화를 하기위한 키(Kc) 값을 생성 완료하고 본 발명의 단말기는 암호화 준비가 다 되었으니 네트워크만 암호화 준비가 되면 된다는 의미이다.

<115> 따라서 본 발명에서는 전송중인 데이타에 암호화를 시키는 과정이 본 발명의 단말기에 의해서 주도적으로 이루어지는 것이다.

<116> 상기 판단(803)결과 수신된 전송중 암호화 요청 메시지에 RAND 값이 포함 되었으면 RAND 값을 이용하여 데이타 암호화에 필요한 키 값을 계산(804)한 다음 전송중 암호화 완료 메시지를 단말기로 전송하면, 상기 단말기는 네트워크로 부터 상기 전송중 암호화 완료 메시지를 수신(805)하고 암호화 절차를 완료(806)한다.

<117> 상기 암호화 절차를 완료(806)한 후 전송되는 모든 데이타는 암호화되어 전송되게 된다.

<118> 상기 판단(803)결과 수신된 전송중 암호화 요청 메시지에 RAND 값이 포함 되어있지 않으면 전송되는 데이타에 암호화를 진행할 것인지 판단(807)한다.

<119> 상기 판단(807)결과 전송되는 데이타에 암호화를 진행하지 않기로 하였으면 데이타 전송 중 암호화 불가 메시지를 단말기로 전송(808)하고 절차를 완료(809)한다

<120> 상기 암호화 불가 절차를 완료(809)한 후 전송되는 모든 데이타는 암호화가 되지않은 상태로 전송되게 된다.

<121> 상기 판단(807)결과 전송되는 데이타에 암호화를 진행하기로 하였으면 RAND(RANDom number) 값을 생성하여 SRES(Signed RESponse) 값을 계산/저장(810) 한 다음 암호화 승인 요청 메시지를 단말기로 전송(811)하되 상기 RAND 값을 포함하여 전송한다.

<122> 상기 단말기는 네트워크로 부터 상기 암호화 승인 요청 메시지를 수신한 다음 암호화 승인 응답 메시지를 네트워크로 전송하면, 상기 네트워크는 단말기로 부터 암호화 승인 응답 메시지를 수신(812)한다.

<123> 여기에는 단말기에서 계산한 SRES 값을 포함한다.

<124> 상기 네트워크는 단말기로 부터 상기 암호화 승인 응답 메시지를 받아서 네트워크에 저장된 SRES 값과 상기 단말기로 부터 전송된 SRES 값을 비교한 후 서로 두 값이 동일한지 판단(813)한다.

<125> 상기 판단(813) 결과 두 값이 서로 동일하지 않으면 전송되는 데이타에 더이상 암호를 사용할 수 없다는 전송중 데이타 암호화 승인 불가 메시지를 단말기로 전송(814)한 후 절차를 완료(815)한다.

<126> 상기 절차 완료(815) 후에는 각종 전송 데이타 암호화 서비스가 불가능하다.

<127> 상기 판단(813) 결과 두 값이 서로 동일하면 전송되는 데이타에 얼마든지 암호를 사용할 수 있다는 전송중 데이타 암호화 승인 가능 메시지를 단말기로 전송(816)한 후 절차를 완료(817)한다.

<128> 상기 절차 완료(817) 후에는 각종 전송되는 데이타는 암호화되어 서비스가 가능하다.

【발명의 효과】

<129> 이상에서 설명한 바와 같이 본 발명은 GSM 방식의 이동통신 단말기에서 사용자의 데이타를 암호화하는 절차를 개선 함으로써 사용자의 데이타를 좀 더 신뢰성 있게 전송이 가능하도록 해주는 효과가 있으며, 뿐만아니라 네트워크에서 일방적으로 결정하는 암호화 과정을 단말기에서도 가능하도록 해줌으로써 단말기 사용자는 아무때나 데이타 전송을 원하는 시점부터 데이타를 암호화 하거나 암호화를 해제하거나 함으로써 전송되는 데이타의 신뢰성을 그만큼 높여주는 효과를 제공해준다.

【특허청구범위】

【청구항 1】

GSM방식의 단말기와 네트워크간에 전송되는 테이타를 암호화 시키는 방법에 있어서,

상기 단말기와 네트워크간에 테이타 전송중 암호화가 필요하면 사용자 단말기는 네트워크에 전송되는 메시지의 암호화를 요청하는 전송중 암호와 메시지 요청단계와,

상기 네트워크는 단말기로 부터 온 전송중 암호화 메시지 요청을 받아 이를 승인하는 메시지를 상기 단말기로 전송해주는 암호화 요청 메시지 승인단계와,

상기 단말기는 네트워크로 부터 온 암호화 요청 메시지 승인에 따라 이에 응답하는 메시지를 네트워크로 전송해주는 암호화 승인 메시지 응답단계와,

상기 네트워크는 단말기로 부터 온 암호화 승인 응답 메시지에 따라 데이타 전송중 암호화가 완료 되었다는 메시지를 단말기로 보내주는 전송중 암호화 메시지 완료단계를 포함하여 이루어진 것을 특징으로 하는 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 2】

청구항 1 항에 있어서,

상기 네트워크의 암호화 요청 메시지 승인단계에 의한 암호화 요청 승인 메시지 속에는 RAND 값이 포함된 것이 특징인 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 3】

청구항 1 항에 있어서,

상기 사용자 단말기가 네트워크에 요청한 데이타 전송중 암호와 메시지 요청 시점은 불특정 시점에 하도록 하고,

단말기와 네트워크간에 데이타가 전송되는 중간에도 요청할 수 있도록 한 것이 특징인 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 4】

청구항 1 항에 있어서,

상기 사용자 단말기가 네트워크에 요청한 데이타 전송중 암호와 메시지 요청은 단말기와 네트워크간에 전송되는 데이타가 없을 경우에도 이루어 지도록한 것이 특징인 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 5】

GSM방식의 단말기와 네트워크간에 전송되는 테이타를 암호화 시키는 방법에 있어서,

단말기가 네트워크로 데이타 전송중 암호화가 필요하면 전송되는 데이타에 암호화를 요청하는 특정 값을 포함해서 보내는 특정값 포함 암호화 요청단계와,

상기 네트워크는 단말기로 부터 받은 상기 특정 값을 바탕으로 암호화 과정에 필요한 키 값을 계산한 후 암호화 과정이 완료 되었다고 단말기에게 통보를 하는 암호화 완료단계와,

상기 암호화 완료 후 단말기와 네트워크는 데이타 전송중 암호화를 시작하게 되는 전송중 암호화단계를 포함하여 이루어진 것을 특징으로하는 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 6】

청구항 5 항에 있어서,

상기 특정 값은 RAND 번호 값을 이용한 것이 특징인 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 7】

청구항 5 항에 있어서,

상기 사용자 단말기가 네트워크에 요청한 데이타 전송중 암호와 메시지 요청 시점은 불특정 시점에 하도록 하고,

단말기와 네트워크간에 데이타가 전송되는 중간에도 요청할 수 있도록 한 것이 특징인 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 8】

청구항 5 항에 있어서,

상기 사용자 단말기가 네트워크에 요청한 데이타 전송중 암호와 메시지 요청은 단말기와 네트워크간에 전송되는 데이타가 없을 경우에도 이루어 지도록한 것이 특징인 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 9】

단말기가 대기상태 또는 전송상태에서 단말기가 네트워크에 지금부터 전송되는 모든 데이타에 암호화를 시작하자고 요청하는 전송중 암호화 요청 메시지 전송단계와,

상기 네트워크는 상기 전송중 암호화 요청 메시지를 받아 이 메시지속에 RAND 값이 포함되었으면 상기 RAND 값을 이용하여 암호화에 필요한 키(Kc)값을 계산한 다음 전송데이타의 암호화를 완료하는 키값 산출단계와,

상기 네트워크는 상기 전송중 암호화 요청 메시지를 받아 이 메시지속에 RAND 값이 포함되어있지 않으면 암호화 진행 여부에 따라 RAND 값을 생성하고 SRES 값을 계산/저장한 다음 암호화가 이루어 졌다는 메시지를 단말기로 전송하는 암호화 승인 메시지 전송단계와,

상기 네트워크는 단말기로 부터 암호화 승인 응답 메시지를 받아 네트워크에 저장된 SRES 값과 단말기에서 전송되어온 SRES 값을 비교하여 동일여부에 따라 전송되는 데이타에 암호화여부를 결정하는 전송데이타 암호화 결정단계를 포함하여 이루어진 것을 특징으로하는 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 10】

청구항 9 항에 있어서,

상기 단말기의 전송중 암호화 요청 메시지를 네트워크로 전송시 단말기는 이미 RAND 값을 기준으로 하여 암호화를 하기위한 키(KC) 값을 생성 완료하고 암호화 준비를 마친 것을 특징으로하는 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 11】

청구항 9 항에 있어서,

상기 네트워크가 단말기로 전송하는 암호화 승인 메시지 속에는 RAND 값이 포함된 것을 특징으로하는 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 12】

청구항 9 항에 있어서,

상기 사용자 단말기가 네트워크에 요청한 데이타 전송중 암호와 메시지 요청 시점은 불특정 시점에 하도록 하고,

단말기와 네트워크간에 데이타가 전송되는 중간에도 요청할 수 있도록 한 것이 특징인 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 13】

청구항 9 항에 있어서,

상기 사용자 단말기가 네트워크에 요청한 데이타 전송중 암호와 메시지 요청은 단말기와 네트워크간에 전송되는 데이타가 없을 경우에도 이루어 지도록한 것이 특징인 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 14】

청구항 9 항에 있어서,

상기 네트워크가 단말기로 부터 수신하는 암호화 승인 응답 메시지 속에는 단말기에서 계산한 SRES 값이 포함된 것을 특징으로하는 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 15】

청구항 9 항에 있어서,

상기 네트워크는 수신된 전송중 암호화 요청 메시지속에 RAND 값이 포함되어있지 않고, 암호화도 진행하지 않기로 하였으면 전송되는 데이타는 암호화가되지 않는다는 메시지를 단말기로 전송하는 암호화 불가 메시지 전송단계를 더 포함하여 이루어진 것을 특징으로하는 GSM 이동통신 시스템의 전송 데이타 암호화 방법.

【청구항 16】

GSM방식의 단말기와 네트워크간에 전송되는 테이타를 암호화 해제 시키는 방법에 있어서,

상기 단말기와 네트워크간에 테이타 전송중 암호화가 필요없으면 사용자 단말기는 네트워크에 전송되는 메시지의 암호화 해제를 요청하는 전송중 암호와 해제 메시지 요청단계와,

상기 네트워크는 단말기로 부터 온 암호화 해제 메시지 요청을 받아 이를 처리하여 승인하는 전송중 암호화 중단 완료 메시지를 상기 단말기로 전송해주는 암호화 중단완료 메시지 승인단계를 포함하여 이루어진 것을 특징으로 하는 GSM 이동통신 시스템의 전송 데이타 암호화 해제 방법.

【청구항 17】

청구항 16 항에 있어서,

상기 사용자 단말기가 네트워크에 요청한 데이타 전송중 암호와 해제 메시지 요청 시점은 불특정 시점으로 하고,

단말기와 네트워크간에 데이타가 전송되는 중간에도 요청할 수 있도록 한 것이 특징인 GSM 이동통신 시스템의 전송 데이타 암호화 해제 방법.

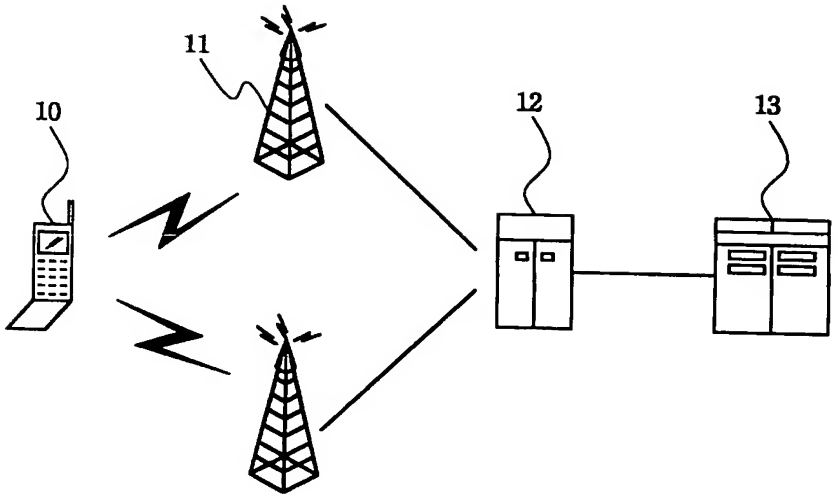
【청구항 18】

청구항 16 항에 있어서,

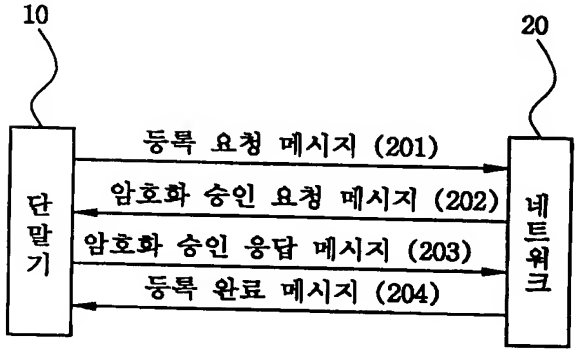
상기 사용자 단말기가 네트워크에 요청한 데이타 전송중 암호와 해제는 단말기와 네트워크간에 전송되는 데이타가 없을 경우에도 이루어 지도록한 것이 특징인 GSM 이동통신 시스템의 전송 데이타 암호화 해제 방법.

【도면】

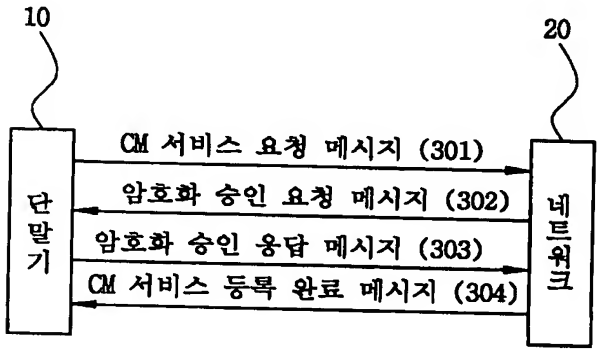
【도 1】


11
10
12
13

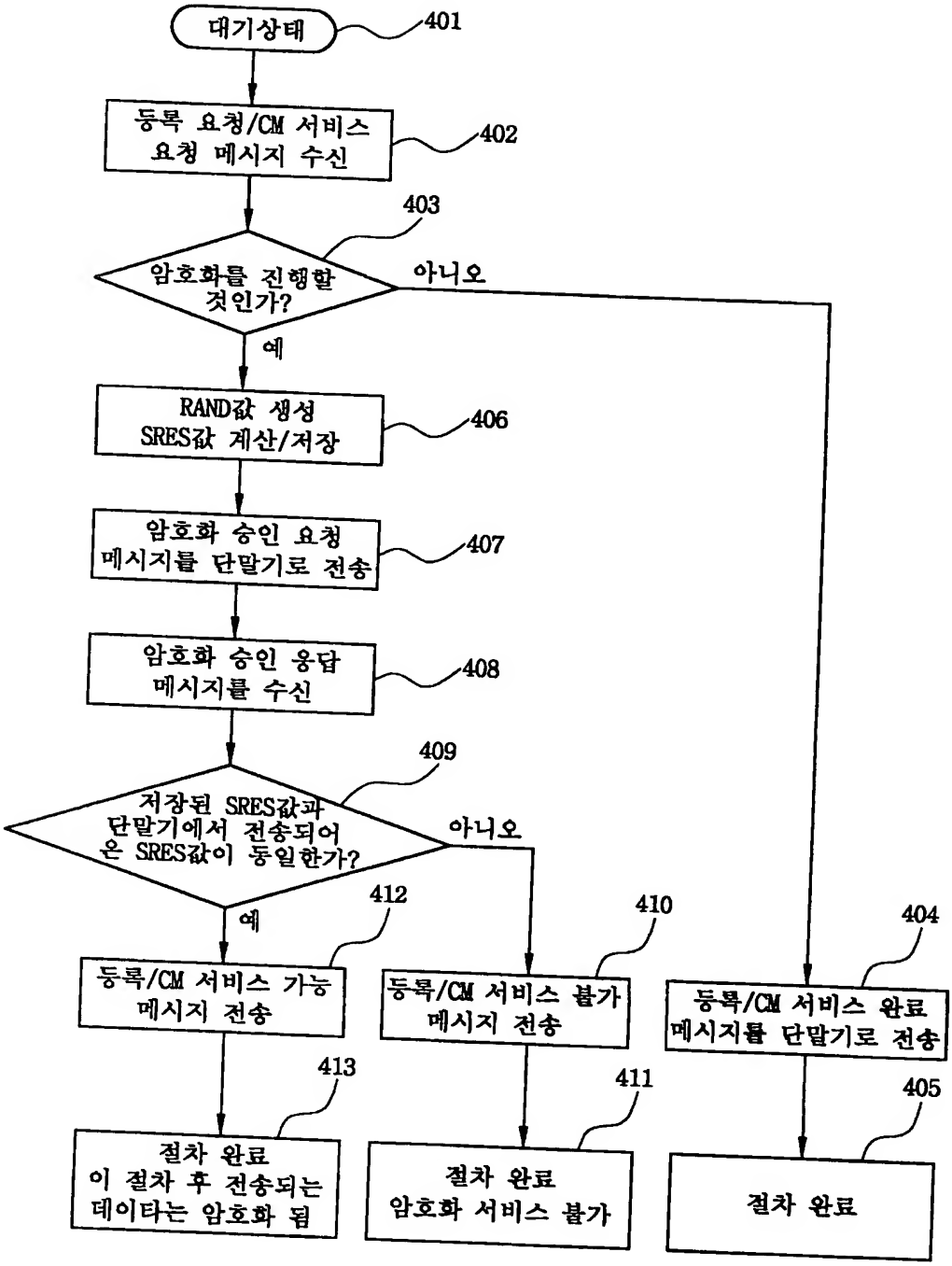
【도 2】


10
20
단말기
네트워크
등록 요청 메시지 (201)
암호화 승인 요청 메시지 (202)
암호화 승인 응답 메시지 (203)
등록 완료 메시지 (204)

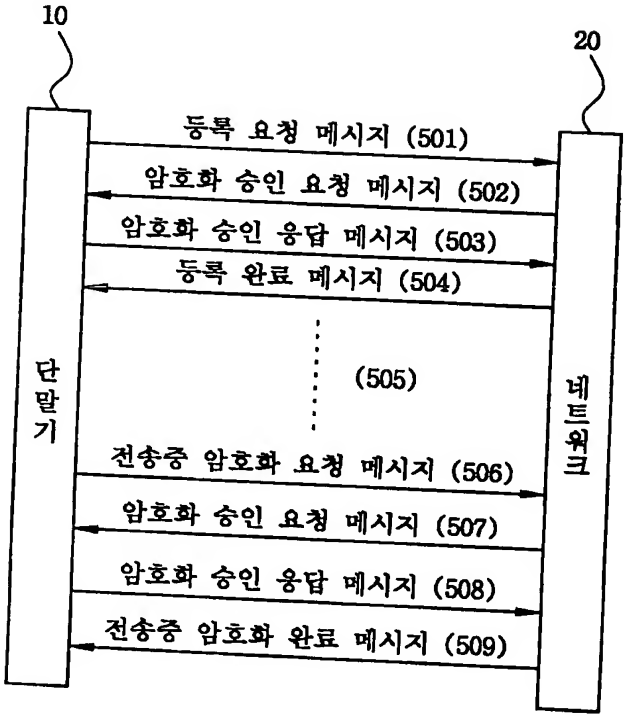
【도 3】


10
20
단말기
네트워크
CM 서비스 요청 메시지 (301)
암호화 승인 요청 메시지 (302)
암호화 승인 응답 메시지 (303)
CM 서비스 등록 완료 메시지 (304)

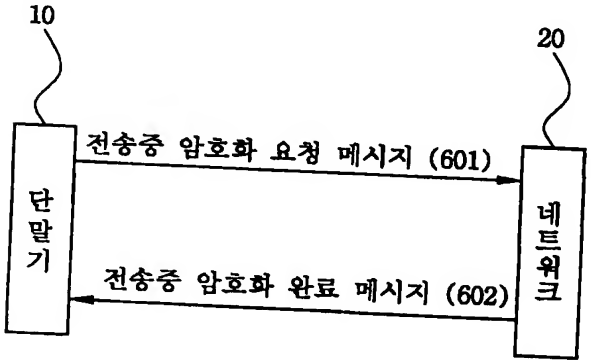
【도 4】


대기상태
401
등록 요청/CM 서비스 요청 메시지 수신
402
403
암호화를 진행할 것인가?
아니오
예
RAND값 생성 SRES값 계산/저장
406
암호화 승인 요청 메시지를 단말기로 전송
407
암호화 승인 응답 메시지를 수신
408
409
저장된 SRES값과 단말기에서 전송되어 온 SRES값이 동일한가?
아니오
예
412
410
404
등록/CM 서비스 가능 메시지 전송
등록/CM 서비스 불가 메시지 전송
등록/CM 서비스 완료 메시지를 단말기로 전송
413
411
405
절차 완료 이 절차 후 전송되는 데이타는 암호화 됨
절차 완료 암호화 서비스 불가
절차 완료

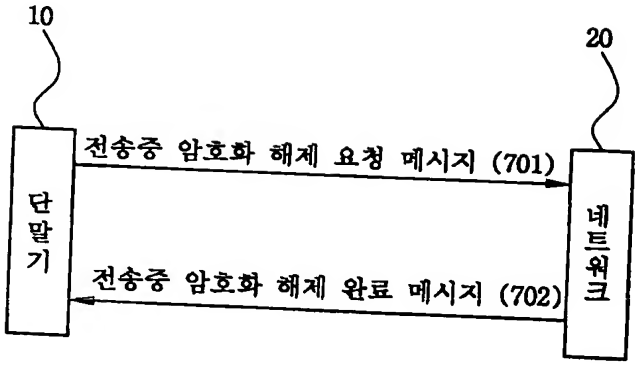
【도 5】


10
20
단말기
네트워크
등록 요청 메시지 (501)
암호화 승인 요청 메시지 (502)
암호화 승인 응답 메시지 (503)
등록 완료 메시지 (504)
(505)
전송중 암호화 요청 메시지 (506)
암호화 승인 요청 메시지 (507)
암호화 승인 응답 메시지 (508)
전송중 암호화 완료 메시지 (509)

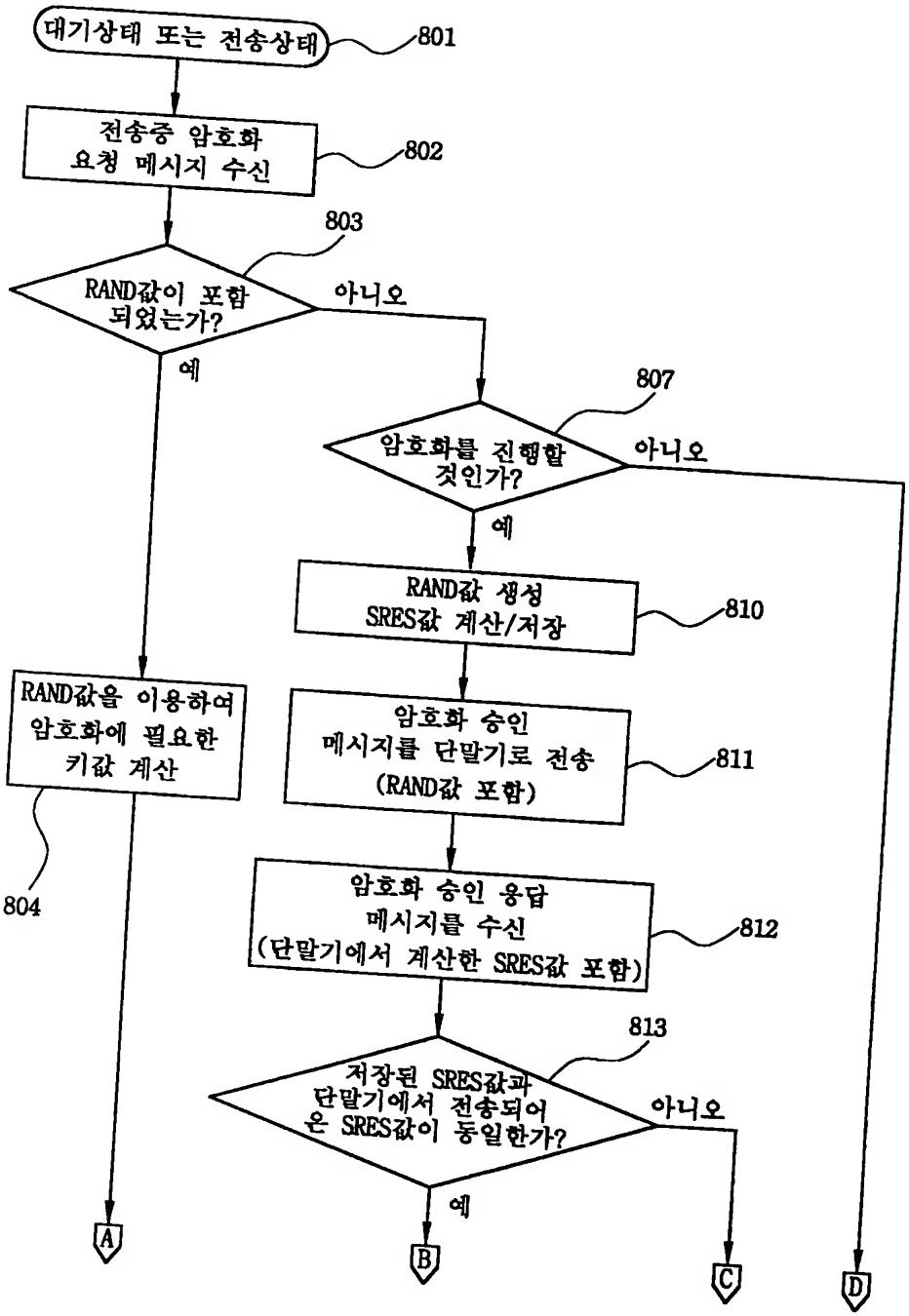
【도 6】


10
20
단말기
네트워크
전송중 암호화 요청 메시지 (601)
전송중 암호화 완료 메시지 (602)

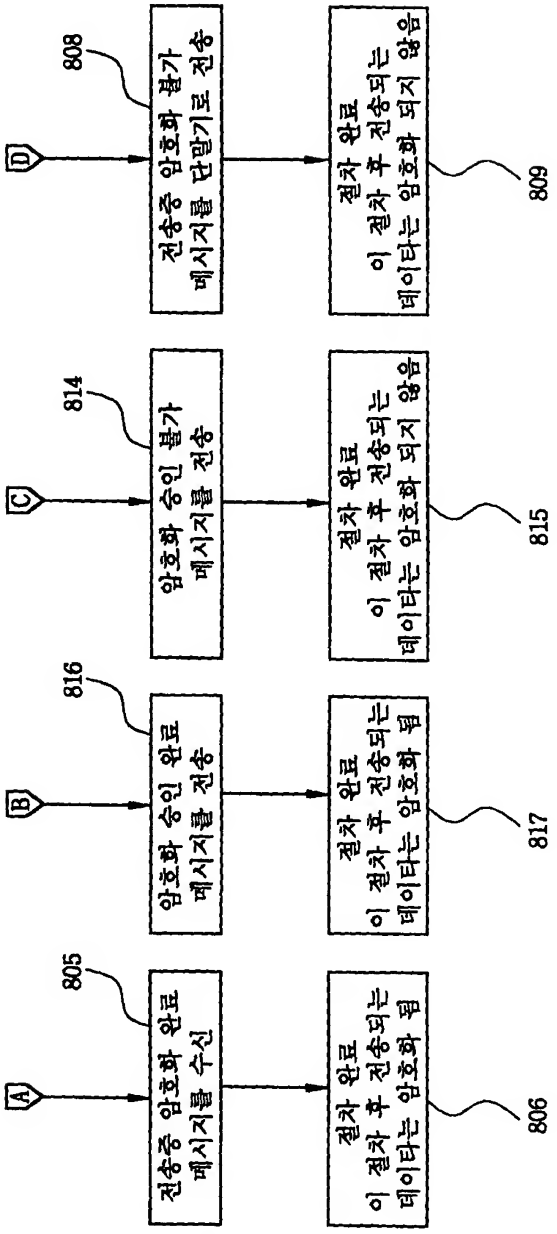
【도 7】



【도 8a】


대기상태 또는 전송상태
801
전송중 암호화 요청 메시지 수신
802
803
RAND값이 포함 되었는가?
아니오
예
807
암호화를 진행할 것인가?
아니오
예
RAND값 생성 SRES값 계산/저장
810
RAND값을 이용하여 암호화에 필요한 키값 계산
804
암호화 승인 메시지를 단말기로 전송 (RAND값 포함)
811
암호화 승인 응답 메시지를 수신 (단말기에서 계산한 SRES값 포함)
812
813
저장된 SRES값과 단말기에서 전송되어 온 SRES값이 동일한가?
아니오
예
A
B
C
D

【도 8b】


A
B
C
D
805
816
814
808
전송중 암호화 완료
메시지를 수신
암호화 승인 완료
메시지를 전송
암호화 승인 불가
메시지를 전송
전송중 암호화 불가
메시지를 단말기로 전송
절차 완료
이 절차 후 전송되는
데이타는 암호화 됨
절차 완료
이 절차 후 전송되는
데이타는 암호화 됨
절차 완료
이 절차 후 전송되는
데이타는 암호화 됨
절차 완료
이 절차 후 전송되는
데이타는 암호화 됨
806
817
815
809